

FIG. 1

PRIOR ART

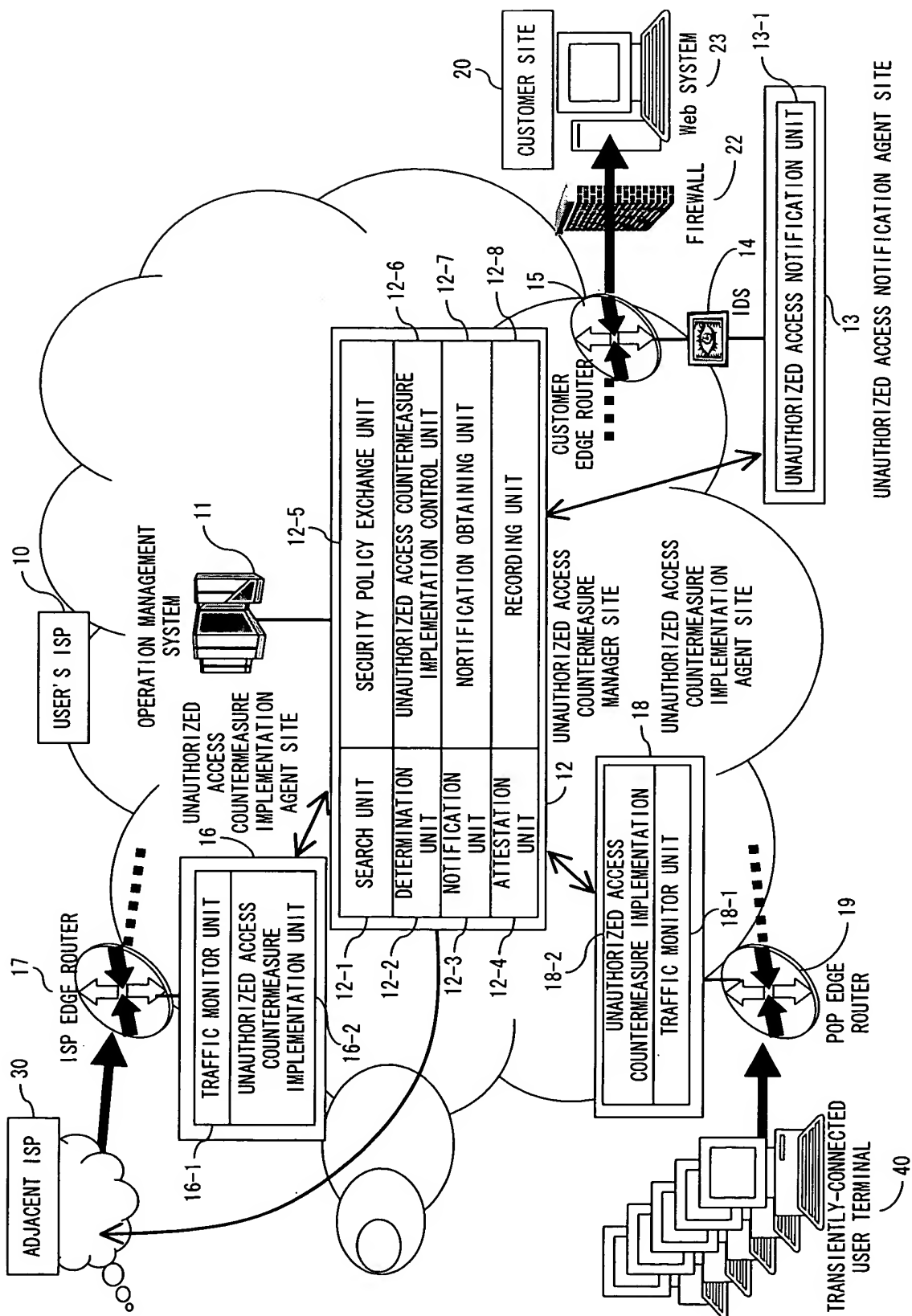


FIG. 2

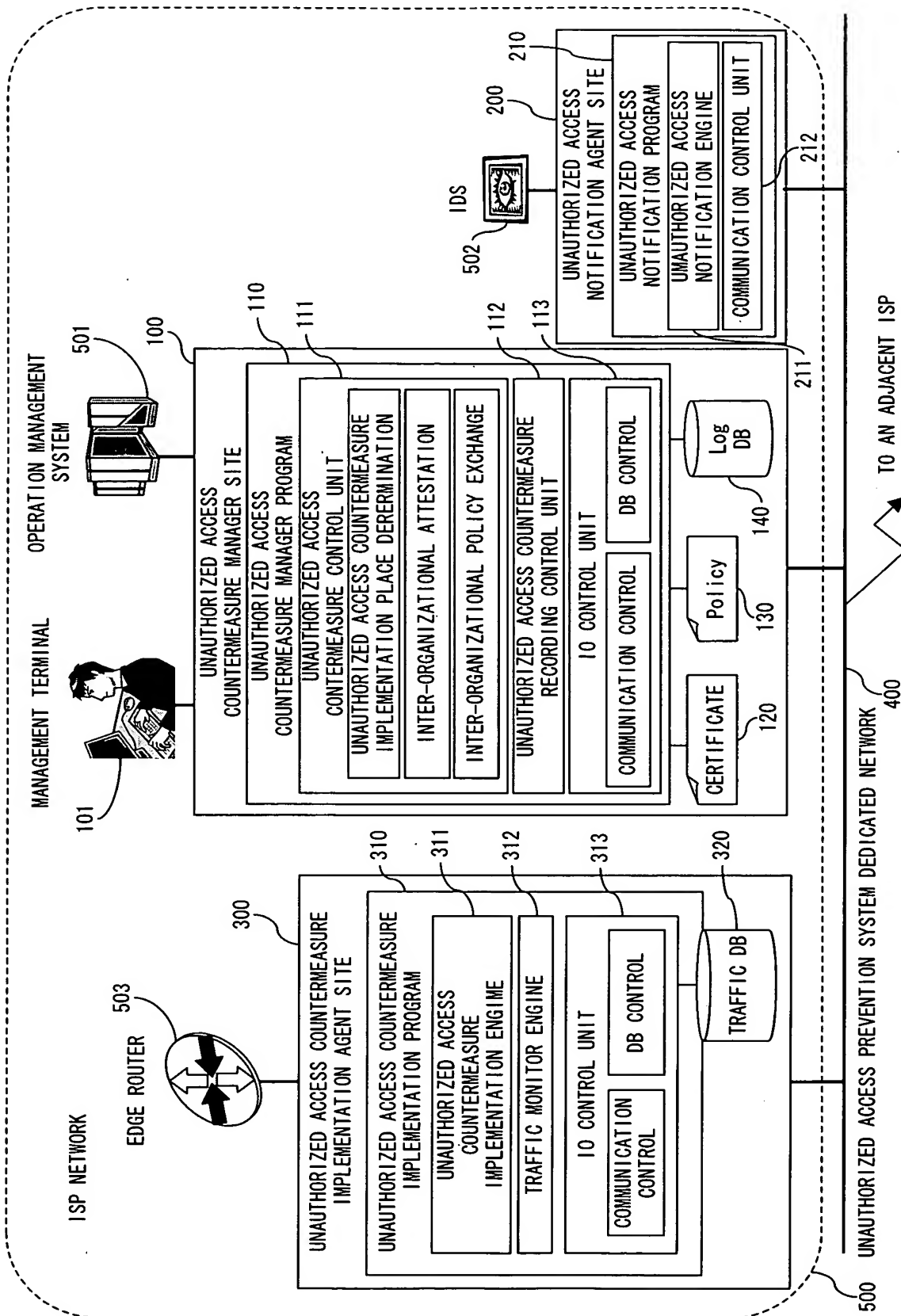


FIG. 3

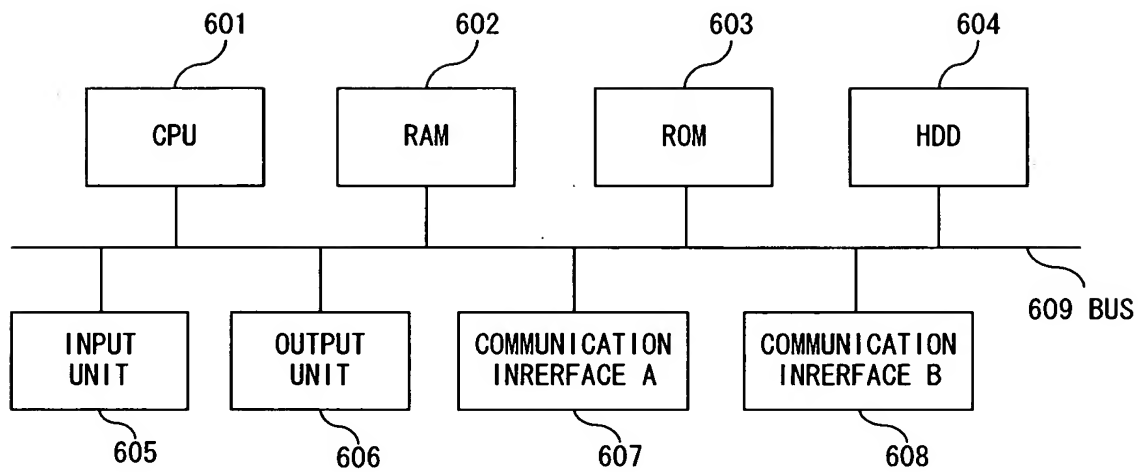


FIG. 4

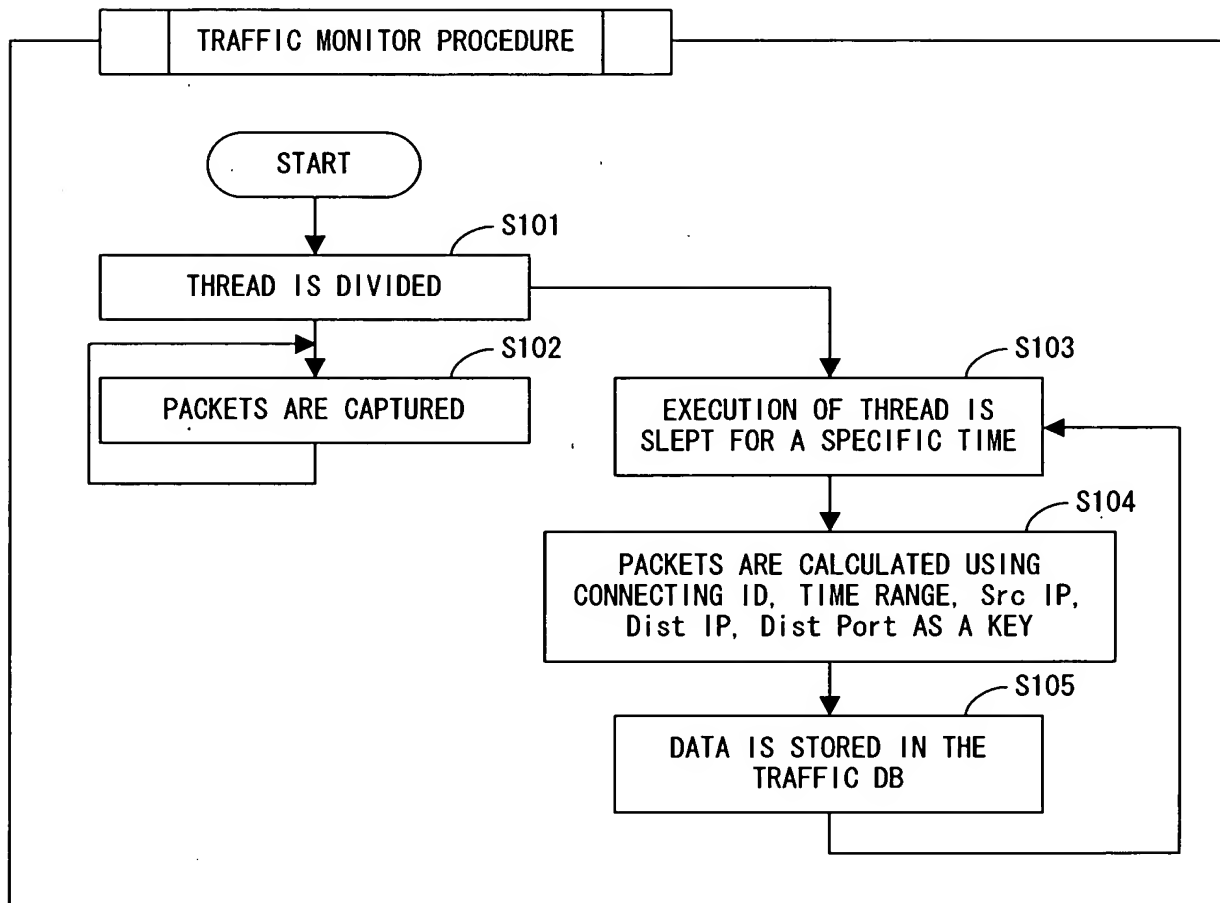


FIG. 5

CONNECTING ID	TIME RANGE	Src IP	Dist IP	Dist Port	Count
ABC01234	10:00-10:10	202.248.20.254	202.248.20.68	80	1456
NBC56780	10:00-10:10	202.248.20.112	202.248.20.68	80	35724
AS245	10:00-10:10	10.34.195.194	202.248.20.68	80	169043

FIG. 6

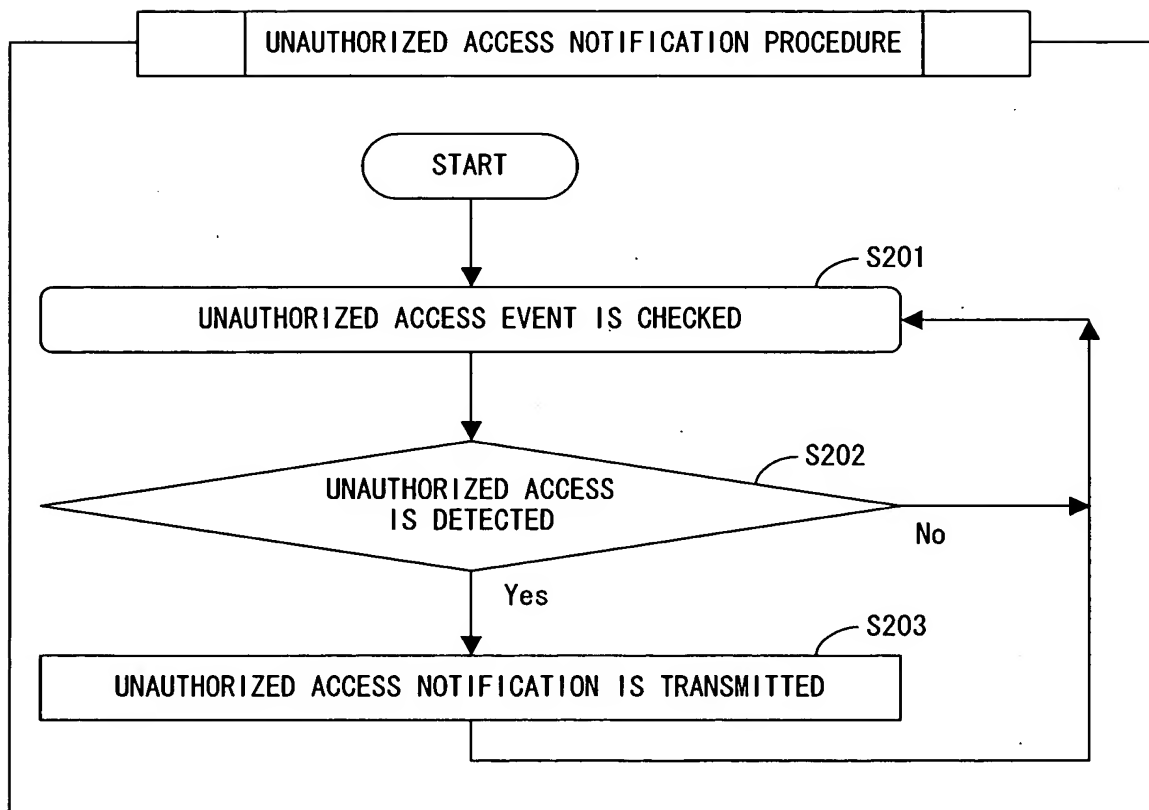


FIG. 7

DATA MEMBER	EXAMPLE 1	EXAMPLE 2
DETECTING ID	00-00-0E-82-2E-74-0001	00-00-0E-82-2E-74-0002
TIME RANGE START (GMT)	2003/2/1 16:01:16	2003/2/17 11:31:11
TIME RANGE END (GMT)	2003/2/1 16:11:16	2003/2/17 11:41:11
ATTACK CATEGORY	TCP Syn Flood	Worm
ORGANIZATION NAME	Company A	Company B
BELONGING ISP	ISP ABC	ISP XYZ
TARGET PROTOCOL	TCP	UDP
Src IP	10. 4. 120. Z	169. 0. 255. C
Dist IP	192. 168. X. Y	164. 71. A. B
Dist Port	80	1434
NUMBER OF UNAUTHORIZED PACKETS	156789	876534
ATTACK TOOL NAME	TFN2K	SQL Slammer
COUNTERMEASURE CANCELLATION POLICY	10 MINUTES	20 MINUTES

F I G. 8



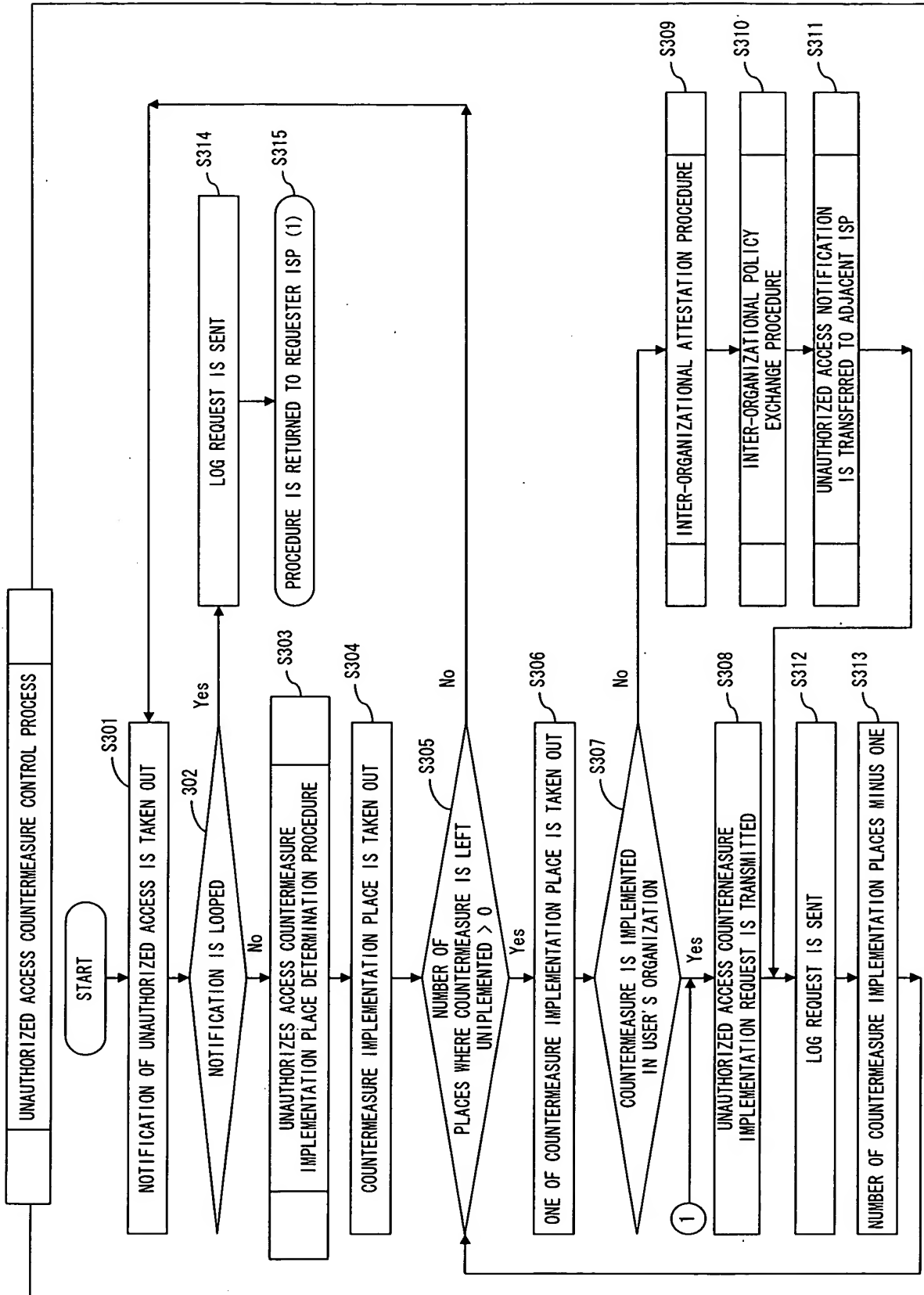


FIG. 9

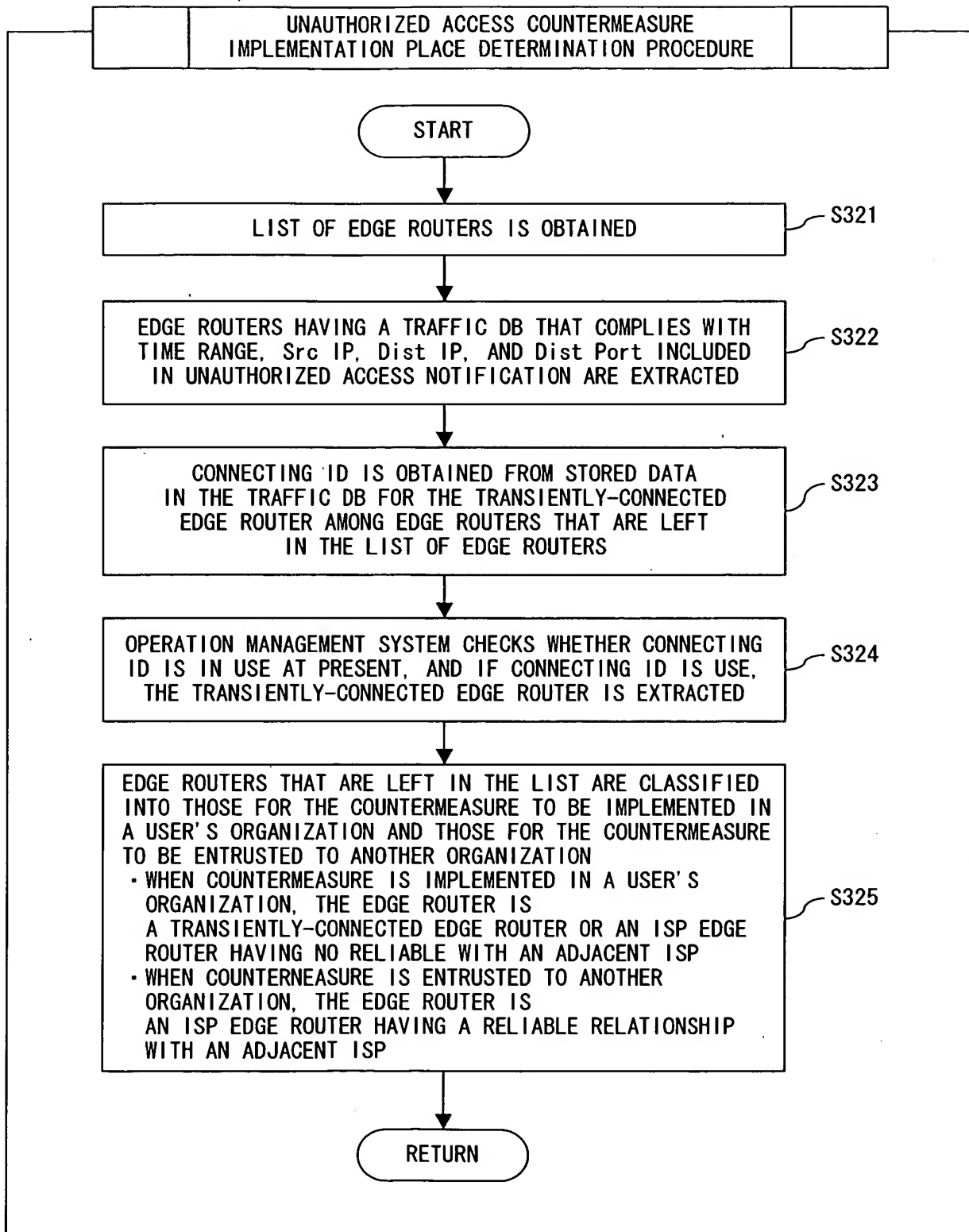


FIG. 10

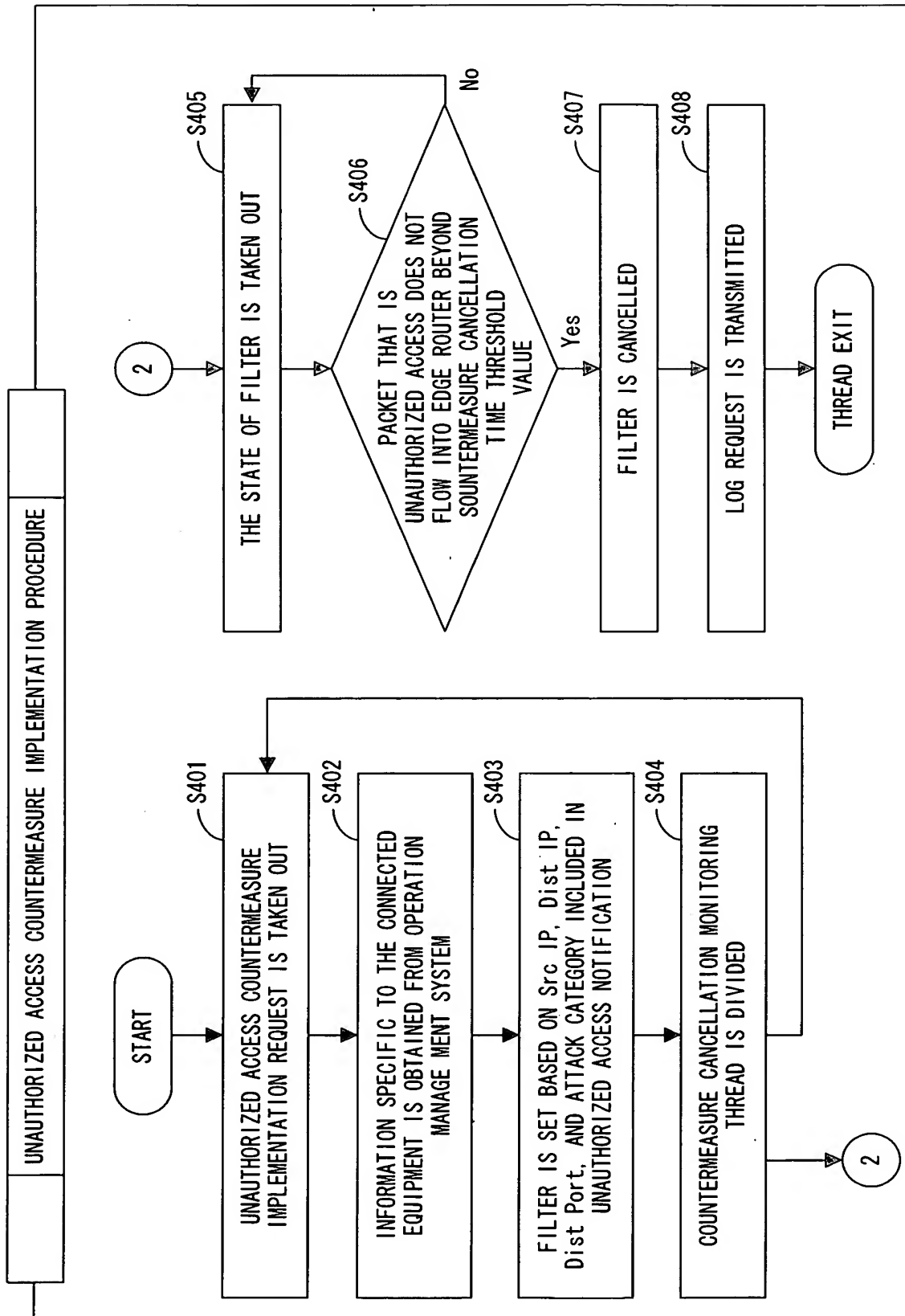


FIG. 11

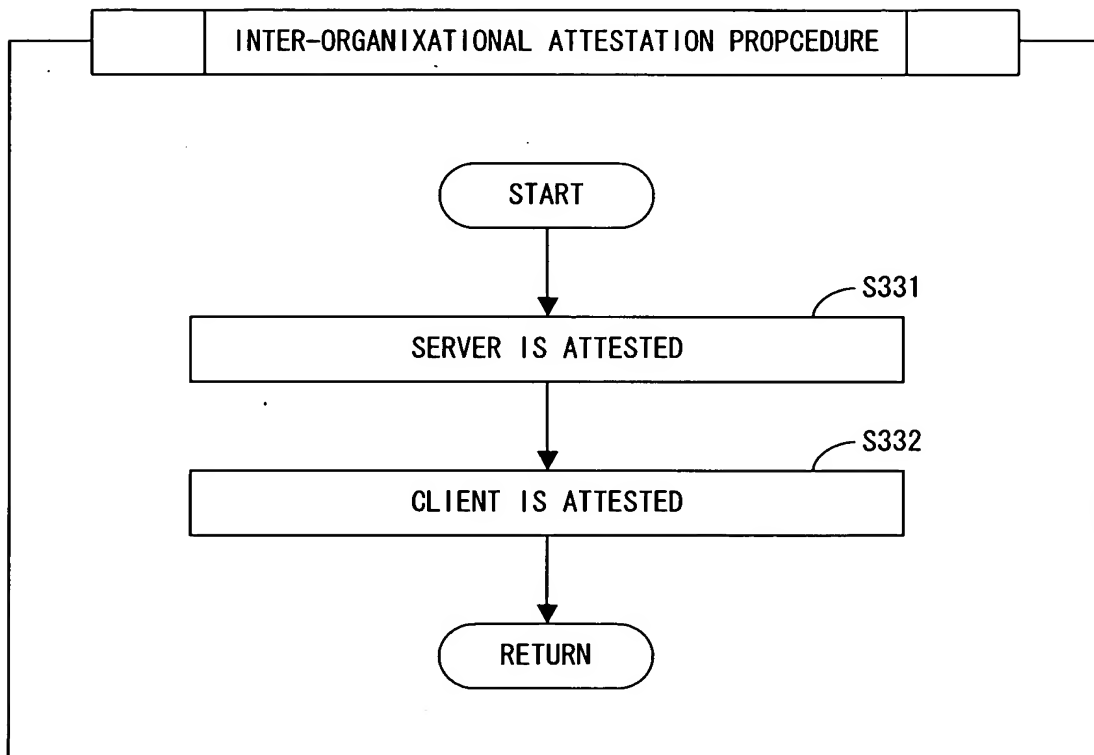


FIG. 12

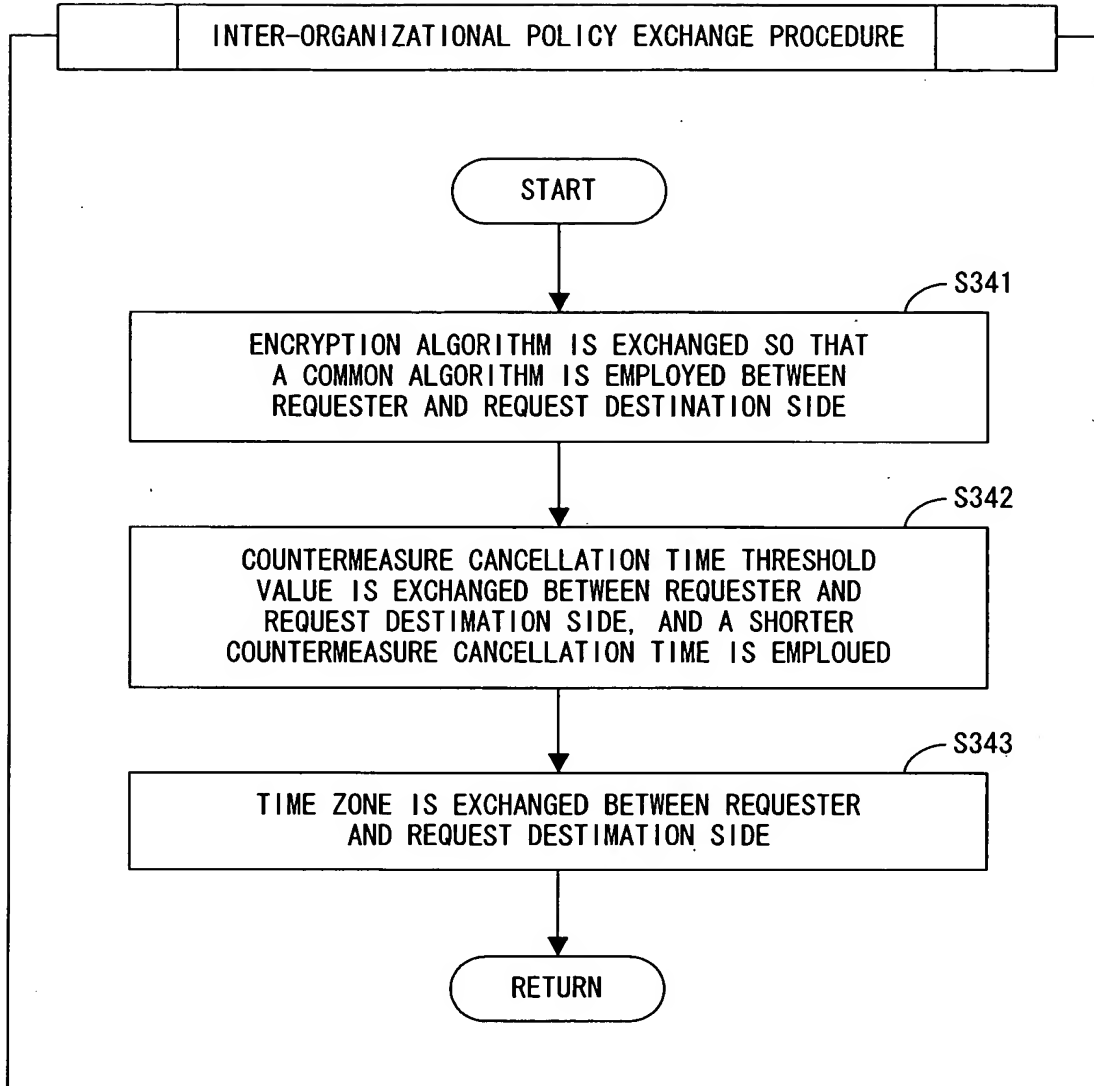


FIG. 13

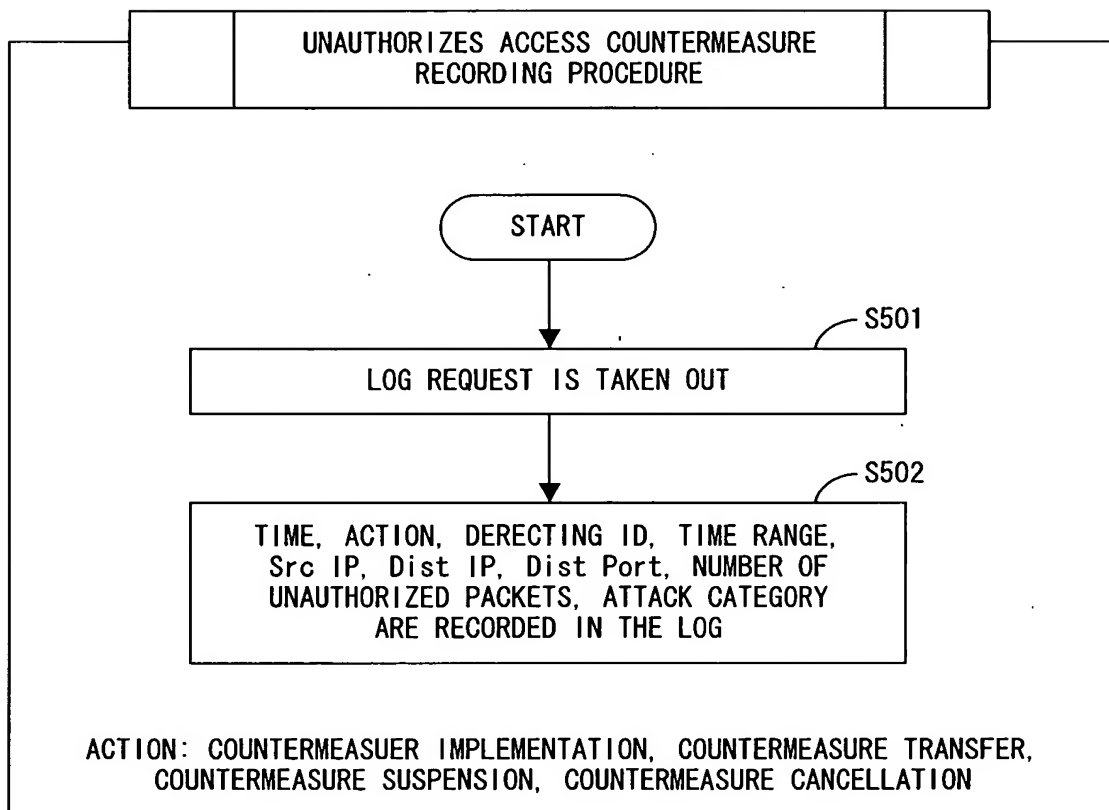


FIG. 14

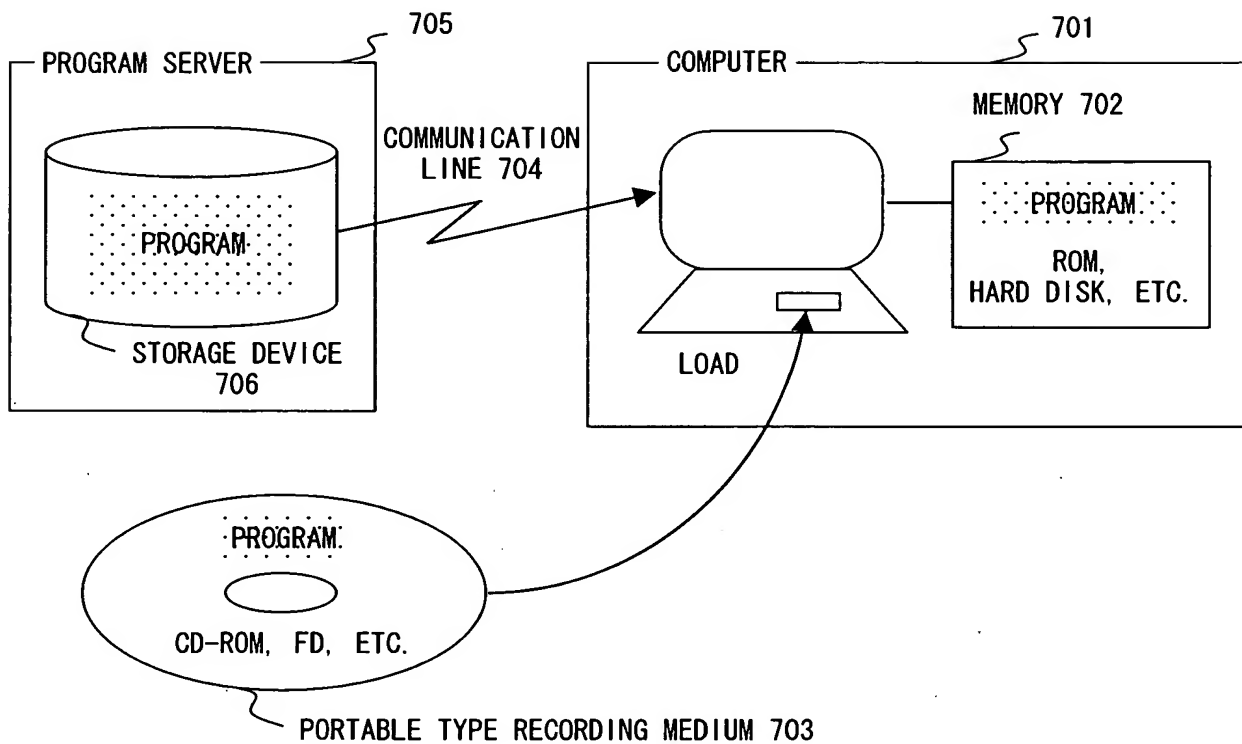


FIG. 15